

Web Application Incident Response & Forensics: A Whole New Ball Game!

Presentation Handout and Quick Reference Sheet

Created by Chuck Willis (chuck.willis@mandiant.com) and

Rohyt Belani (rohyt.belani@intrepidusgroup.com)

Presented at Black Hat Briefings DC 2007 on February 28, 2007

Slides available at www.blackhat.com.

Key Files To Obtain And Analyze When Responding To A Web Application Incident

Note: The filenames and paths below are the default values. Keep in mind that many log file names and locations can be changed in the application configuration. Log file names and location may also change between versions of a software product.

Web Server Logs

- IIS
 - IIS logs stored in LogFiles\W3SVCx
 - URLScan logs will be in the same directory as URLScan if it is in use
- Apache
 - Access log – access.log on Windows, access_log on Unix
 - Error log – error.log on Windows, error_log on Unix
 - ModRewrite Log – if in use and logging, writes to rewrite.log

Application Server Logs

- ASP.NET
 - Does not have its own log files
 - Events are sent to OS event log
- BEA WebLogic
 - Server log – DOMAIN_NAME/servers/SERVER_NAME/logs/SERVER_NAME.log
 - Domain log – DOMAIN_NAME.log
 - Other logs may be present and location varies:
 - HTTP Log
 - Same format as Apache access log
 - May not have the filename access_log or access.log
 - Can be configured for log rotation with a sequence number or timestamp in the filename
 - Node Manager Log – NODE_MANAGER_HOME/nodemanager.log

- BEA WebLogic – other logs (continued)
 - Node Manager Server Instance Log – DOMAIN_NAME/servers/ SERVER_NAME/logs/SERVER_NAME.out
 - Standard Output and Standard Error
 - Not enabled by default
 - No default filenames
 - Set in WebLogic startup script
 - Java Transaction API (JTA) Log
 - Used for ensuring transactions complete, not recording them
 - SERVER_NAME0000.tlog, SERVER_NAME0001.tlog, etc
 - Heuristic Transaction Log files may also exist named SERVER_NAME0000.heur.tlog, etc.
 - Java Database Connectivity (JDBC) Log – SERVER_NAME/jdbc.log
- IBM WebSphere
 - Apache Access Log – access.log or access_log
 - Apache Error Log – error.log or error_log
 - IBM Service Log – activity.log
 - Java Virtual Machine Logs – SystemOut.log and SystemErr.log
 - Process Logs – native_stdout.log and native_stderr.log

Database Server Logs

- Microsoft SQL Server
 - Writes login, logout, and some other activity to the OS Application event log
 - Error Log
 - Stored in \Mssql\Log
 - Current log filename is simply ErrorLog (no extension)
 - Six previous logs stored by default with names ErrorLog.1 (most recent) to ErrorLog.6 (oldest)
 - Server Side Traces can be configured to log data – location of log varies depending on how traces were configured
 - If C2 Auditing is in use, logs are stored in files named audittrace_*.trc in the database data directory
- Oracle
 - Database startup, shutdown, and connection with administrator privileges logged to the OS log by default
 - Additional events can be stored in the OS log or in a database table
 - Alert log – alert.log – Errors, messages, and trace file references
 - Trace files
 - Result from an error or from administrator action
 - Named *ora*.trc (depends on configuration and OS)

Application Logs

- Events logged and the location of logs files is entirely dependent on the application
- Ask developers or administrators:
 - Where are application logs?
 - What is format?
 - What messages would result from likely malicious activity?
 - How long are logs stored?